**REMARKS**

This Amendment is in response to the Office Action dated September 12, 2006 ("OA"). In the Office Action, claim 30 was objected to, claims 30 and 33-36 were rejected under 35 USC §102(b) and claims 31, 32, 37 and 38 were rejected under 35 USC §103(a). By this Amendment, claims 30 and 33 are amended. Claims 30-38 are believed allowable, with claim 30 being an independent claim.

CLAIM OBJECTIONS:

Claim 30 was objected because it contained a misspelling of the word "from". OA, pg. 2. By this amendment, the word "form" has been amended to "from". It is noted that while the Examiner states that the error existed in claim 1, it is evident that the Examiner intended to refer to claim 30 in light of the fact that claim 1 has been cancelled. The Applicants thank the Examiner for pointing out this typographical error.

CLAIM REJECTIONS UNDER 35 USC §102:

Claims 30 and 33-36 were rejected under 35 USC §102 as being anticipated by Norton Antivirus for Windows 95/98 User's Guide (hereinafter "Norton"). To anticipate a claim, the reference must teach every element in the claim. MPEP 2131. Under an anticipation rejection, the identical invention must be shown in as complete detail as is contained in the claim. MPEP 2131 citing *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

Claim 30:

Claim 30 is amended herein to recite, in part, "an activation token identifying system characteristics and specifying a threat level and at least one preset activation measure, wherein a system characteristic is one of the group of a hardware system, a service, a configuration of a service, a service execution platform, and a service version." Support for this amendment can be found at least at paragraphs 16-18 and 30 of the application. Thus, no new matter is believed to be introduced by this amendment.

The above-cited element of claim 30 not only requires the existence of an activation token but also imposes several limitations on the contents of the activation token. The system characteristic identified by the activation token must be one of the listed types. The activation token must specify a

threat level. It is noted that because the activation token identifies specific system characteristics, the specified threat level is thus associated with the system characteristic. Furthermore, the activation token must specify at least one preset activation measure. It is likewise noted that because the activation token identifies specific system characteristics, the at least one preset activation measure is thus associated with the system characteristic.

Claim 30 additionally recites, in part, "a first system configured to at least review security and vulnerability information from information publishers and to provide the activation token based on the security and vulnerability information." Thus, claim 30 also requires that the activation token be based on security and vulnerability information from information publishers.

In rejecting claim 30, the Examiner alleges that "Norton discloses a security system comprising: an activation token identifying system characteristics and specifying a threat level and at least one preset activation measure (see pages 37-40)." OA, pg. 6. The Applicants respectfully submit that Norton does not disclose an activation token which identifies a system characteristic of a type listed in claim 30, specifies a threat level, specifies at least one preset activation measure and is based on security and vulnerability information from information publishers.

The passage cited by the Examiner discloses transmitting "virus definitions files" from a first computing system to a second computing system. Norton, pg. 37. The cited passage is primarily concerned with the mechanics of transmitting the virus definitions files. Absent from the cited passage or any other discussion of the virus definitions files in Norton is a precise description of the contents of the virus definitions files. In particular, no mention is made of the virus definition files specifying a threat level. Nor is any mention made of the virus definition files specifying at least one preset activation measure. As previously noted, claim 30 requires an activation token including specific content. The Applicants respectfully submit that the virus definitions files taught by Norton cannot teach these limitations because their content is not expressly stated.

The Applicants additionally submit that "virus definitions files" mentioned in Norton fails to suggest the specific limitations required by claim 30. Norton states, "Norton AntiVirus safeguards your computer from

virus infection, no matter what the source" and instructs the user to "install the latest virus definitions." Norton, pg. 16 and 40. Norton discloses,

> Regularly obtain from Symantec updated information that Norton AntiVirus needs to keep your virus protection up-to-date . . . . New viruses are being written all the time. You have to regularly obtain files from Norton AntiVirus that contain the latest virus protection. If you don't, you are not protected against viruses that have been released into the computer world since you bought the product. Norton, pg. 16.

As previously noted, Claim 30 requires an activation token identifying a system characteristic. Furthermore, the system characteristic must be one of the group of a hardware system, a service, a configuration of a service, a platform on which a service executes and a version of a service. As the term is used in the art, a computer virus is a computer program written to alter the way a computer operates, without the permission or knowledge of the user. See http://en.wikipedia.org/wiki/Computer_virus (December 11, 2006). Norton concurs, defining viruses as follows: "A computer virus is, simply, a computer program written by an ill-intentioned programmer." Therefore, a virus is not inherently a member of the group of a hardware system, a service, a configuration of a service, a platform on which a service executes and a version of a service.

Additionally, as previously noted, claim 30 requires that an activation token must specify a threat level. The Applicants respectfully submit that Norton does not teach or suggest an activation token specifying a threat level.

The American Heritage® Dictionary of the English Language, Fourth Edition, defines the word "level" as "[r]elative position or rank on a scale." Houghton Mifflin Company, 2000 (http://dictionary.reference.com/browse/level). Furthermore, this definition is the first of several definitions provided. By convention, dictionaries list more common or important definitions for words first. It is noted in this definition that positions are defined relatively to each other. Relativeness, by definition, comprises comparing an entity to other entities. It therefore follows that at least two levels must exist.

Furthermore, this interpretation of the meaning of "threat level" is consistent with the term's usage within the specification. The specification

discloses an exemplary scale of threat levels which specify the severity of the threat associated with an activation token:

> The activation information could be just a degree of vulnerability respectively a threat level. An example of a set of threat levels characterizes threat levels from 1 to 5. Level 1 characterizes a possible service degradation by a vulnerability that allows an adversary to decrease the performance of the system significantly. Level 2 characterizes a possible denial of a service by any kind of vulnerability that allows an adversary to tamper with the system so it becomes unavailable. Level 3 characterizes a possible information theft by any kind of vulnerability that allows an adversary to obtain supposedly secret information. Level 4 characterizes a possible information manipulation by any kind of vulnerability that allows an adversary to manipulate or inject data into a system. Level 5 characterizes a possible taking control of a system by any kind of vulnerability that allows an adversary to execute arbitrary code on a system and therefore to compromise a system. App., para. 0012.

Absent from Norton is a teaching that a specific virus is categorized into one of two or more levels. To the contrary, Norton instructs users of Norton AntiVirus that "For a VIRUS FOUND, Repair is always the best choice." Norton, pg. 28. This instruction suggests an absence of treating viruses differentially based on their severity.

Additionally, as previously noted, claim 30 requires that an activation token must specify at least one preset activation measure. The Applicants respectfully submit that Norton does not teach or suggest an activation token specifying at least one preset activation measure.

Norton specifies a plurality of measure which may be taken in response to a virus. These actions include "Repair", "Delete", "Stop", "Continue", "Exclude", "Inoculate" and "Quarantine." Norton, pg. 28. Norton clarifies that the user may select which action to take: "Press Enter to choose the action that is preselected for you, or type the first letter of the action you want to take (for example, type R for Repair)." Norton, pg. 26. As previously noted, claim 30 requires a preset activation measure specified in an activation token based on security and vulnerability information from information publishers. By contrast, a human being does not, and cannot feasibly be required to, base his or her decisions on information from information publishers. Therefore, an action by a human being cannot meet this requirement of claim 30. Furthermore, absent from Norton is any teaching that available measures or a default measure are specified in the virus definitions files.

For at least these reasons, the Applicants respectfully submit that claim 30 is not anticipated by Norton and earnestly solicit allowance of the claim.

Claim 33:

Claim 33 recites, "The system of claim 30, wherein the first system is further configured to automatically filter the security and vulnerability information relevant to the system characteristics identified by the activation token." It is noted that claim 33 is dependent on and further limits claim 30.

Support for the amendments to claim 33 can be found at least at paragraph 24 of the application. As noted in the specification, "In order to facilitate the work done by the administrator, the reviewing means 5 could as well include filtering means for automatic filtering information in respect of specific systems." App., para. 0024. Thus, filtering is performed to extract, from a larger body of information, only that information relevant to a specific system. For example, a first system may provide activation tokens to a group of second systems which is heterogeneous (the second systems may vary in their system characteristics). As such, a specific activation token may or may not be relevant to a specific second system.

The Applicants respectfully submit that Norton contains no teaching or suggestion of providing different virus definitions files or information to different systems based on the characteristics of those systems.

For at least these reasons, and those given for claim 30, the Applicants respectfully submit that claim 33 is not anticipated by Norton and earnestly solicit allowance of the claim.

Claims 34-36:

Claims 34-36 are dependent on and further limit claim 30. Since claim 30 is believed allowable, claims 34-36 are also believed allowable for at least the same reasons as claim 30.

CLAIM REJECTIONS UNDER 35 USC §103:

Claim 31 was rejected under 35 USC §103 as obvious over Norton in view of U.S. Patent No. 6,721,721 to Bates et al. (hereinafter "Bates").

Claims 32 and 38 were rejected under 35 USC §103 as obvious over Norton in view of U.S. Patent No. 6,636,983 to Levi (hereinafter "Levi").

Claim 37 was rejected under 35 USC §103 as obvious over Norton in view of U.S. Patent No. 6,651,249 to Waldin et al. (hereinafter "Waldin").

Claim 31:

Claim 31 recites, "The system of claim 30, further comprising a cryptographic means configured to verify at the second system that the first system is a trusted service." It is noted that claim 31 is dependent on and further limits claim 30.

It is noted that while the Examiner stated that the argument applies to claim 32, it is evident that the Examiner intended to refer to claim 31. The specific arguments raised concern limitations of claim 31.

In rejecting claim 31, the Examiner acknowledges that "Norton fails to disclose cryptographic means configured to verify at the second system that the first system is a trusted service." OA, pg. 5. However, the Examiner states that Bates "teaches the use of cryptographic verification." *Id.* The Examiner alleges that the motivation to combine the virus removal method taught by Norton and the cryptographic verification method taught by Bates "would have been to authenticate the information and the sender of the information." *Id.* The Applicants have reviewed Bates and respectfully disagrees with the Examiner's conclusions.

To establish a *prima facie* case of obviousness, there must be some suggestion or motivation to modify the reference or to combine reference teachings. MPEP 2143. When determining obviousness, "the [E]xaminer can satisfy the burden of showing obviousness of the combination 'only by showing some objective teaching in the prior art or that knowledge generally available to one of ordinary skill in art would lead that individual to combine the relevant teachings of the references.'" In re Lee, 277 F.3d 1338, 1343, 61 USPQ2d 1430, 1434 (Fed. Cir. 2002), citing In re Fritch, 972 F.2d 1260, 1265, 23 USPQ2d 1780, 1783 (Fed. Cir. 1992). "Broad conclusory statements regarding the teaching of multiple references, standing alone, are not 'evidence.'" In re Dembiczak, 175 F.3d 994, 999, 50 USPQ2d 1614, 1617 (Fed. Cir. 1999). "Mere denials and conclusory statements, however, are not sufficient to establish a genuine issue of material fact." Dembiczak, 175 F.3d at 999, 50 USPQ2d at 1617, citing McElmurry v. Arkansas Power & Light Co., 995 F.2d 1576, 1578, 27 USPQ2d 1129, 1131 (Fed. Cir. 1993).

The LiveUpdate method taught by Norton comprises connecting to a specific, known server on the Internet. In the section "Updating virus

protection with LiveUpdate", Norton states that "Norton AntiVirus connects to a special Symantec site on the Internet." Norton, pg. 37. It is emphasized that the Internet site is operated by Symantec Corporation, which is the author of the Norton AntiVirus software. It follows that the Internet site can be trusted because it is operated by a known entity. It further follows that information transmitted from the Internet site can be trusted because it originates from a trusted site. Because both the information and the sender of the information can be trusted, no motivation exists to perform additional methods to authenticate the information and the sender of the information.

For at least these reasons, the Applicants respectfully submit that claim 31 is not obvious over Norton in view of Bates and earnestly solicit allowance of the claim.

Claims 32, 37 and 38:

Claims 32, 37 and 38 are dependent on and further limit claim 30. Since claim 30 is believed allowable, claims 32, 37 and 38 are also believed allowable for at least the same reasons as claim 30.

**CONCLUSION**

In view of the forgoing remarks, it is respectfully submitted that this case is now in condition for allowance and such action is respectfully requested. If any points remain at issue that the Examiner feels could best be resolved by a telephone interview, the Examiner is urged to contact the attorney below.

No fee is believed due with this Amendment, however, should such a fee be required please charge Deposit Account 50-0510 the required fee. Should any extensions of time be required, please consider this a petition thereof and charge Deposit Account 50-0510 the required fee.

Respectfully submitted,

Dated: December 11, 2006

Ido Tuchman, Reg. No. 45,924
Law Office of Ido Tuchman
82-70 Beverly Road
Kew Gardens, NY 11415
Telephone (718) 544-1110
Facsimile (718) 544-8588